NFV ORCHESTRATION, INFRASTRUCTURE AND VNF

Multi-Vendor Interoperability Showcase 2017

EANTC

EDITOR'S NOTE

Results of the first NIA MANO interop test campaign show that only the basic NFV management concepts are interoperable; any serious scaling, resource, and fault management mechanisms are too complex and too vaguely defined to interoperate. Likewise, the northbound orchestration APIs lack definitions, seriously hampering automated testing required in the DevOps model. The industry as a whole needs to rethink interoperability goals and how to achieve them.

What is "Interoperability"? What can we expect? And what level of NFV interoperability will service providers need, after all?

Carsten Rossenhövel
Co-Founder & CTO, EANTC

The more our team at EANTC has tested multi-vendor Network Functions Virtualization (NFV) solutions, the more we are asking ourselves such basic questions.

Almost four years have passed since our very first public NFV showcase in October 2013. We have progressed standardization of interoperability test guidelines within ETSI, most recently the TST007 work item for NFV management and orchestration (MANO) interoperability testing. On behalf of the New IP Agency, we have tested interoperability of virtualized network functions (VNFs) with infrastructure (NFVI) since November 2015.

In parallel, the whole industry has worked hard to standardize procedures, develop open source (OpenStack, OPNFV and others) and commercial solutions.

Still, multi-vendor NFV interoperability does not come easy. This white paper reports the results of our MANO, NFVI and VNF test campaign and showcase prestaged at EANTC's lab in Berlin, Germany between April 24 to May 5.

From an operator view, we covered the standard life cycle functions — setting up, managing, scaling and tearing down service chains as a service provider network operations center (NOC) would need to do on a daily basis. From a vendor view, however, we attempted some really difficult and cumbersome integration with third parties — something that takes substantial lead time and is often a custom integration task.

This is the second MANO interop test open to the whole industry, following the first ETSI NFV Plugtest in January 2017. EANTC participated in the ETSI Plugtest and co-authored the test guidelines (TST007). While ETSI headlined their Plugtest results were "outstanding", the public press release warned that any combinations trying non-basic interoperability "showed that there is still work to be done." Yes, we can (unfortunately) confirm the statement.

NFV orchestrators and VNFs often took a lot of time to integrate; any non-trivial scaling and healing tests worked in fewer combinations due to limited implementation support with most implementations, automated northbound control of the NFV orchestrators turned out to be an investigative undertaking due to incomplete or outdated documentation or conceptual issues of NFVO control.

In the end, we covered 55 test combinations including a few advanced network service scaling, VNF scaling and network service healing cases. These amount to 17 % of the theoretically possible combinations – work to be completed in the future. The successfully completed test combinations yielded a lot of data documented on the following pages.

NIA takes pride in publishing detailed, transparent results which enable the industry to understand the reasons, background and lessons learned in more detail. I hope you will enjoy the read. [summary]

TABLE OF CONTENTS

INTRODUCTION

In 2015, EANTC on behalf of the New IP Agency evaluated a multi-vendor Network Function Virtualization (NFV) Infrastructure to Virtual Network Function (VNF) interoperability. While the test results showed that remarkable progress has been made in the network virtualization implementation, there were still many challenges that needed to overcome before an industrial NFV deployment. Among them, the NFV management and orchestration (MANO) has got special attention. NFV MANO is a working group (WG) of the European Telecommunication Standard Institute (ETSI) that addresses this challenge by defining frameworks for the management and orchestration of all resources in a cloud environment. The main focus of the NFV MANO is to allow flexible network service life cycle management, thus elimi-

nating some issues that can be associated with the rapid provisioning of network components. Although a significant progress has been made by the ETSI in defining the NFV MANO frameworks, managing and orchestrating resources in a multi vendor environment remain challenging.

In this year, the testing focussed on the early interoperability assessment of MANO solutions, which included the NFV orchestrator (NFVO) and the virtual network function manager (VNFM) with VNFs and NFV Infrastructure (NFVI) from different vendors.

PARTICIPANTS AND PRODUCTS

Vendor	VNF/ NFVI/ MANO	Products
Adva	NFVI, MANO	Adva Ensemble, Adva Ensemble
Fortinet	VNF	FortiGate-VM
Huawei	NFVI	FusionSphere
Juniper Networks	NFVI, MANO, VNF	Juniper Contrail Cloud Platform, Juniper Contrail Service Orchestration, vSRX
Procera	VNF	PacketLogic
Spirent Communications	VNF	TestCenter, CloudStress
ZTE	NFVI, MANO	TECS, vManager

Test Coverage

During the NFV MANO interoperability evaluation, we focussed on the test cases in section 7.6 (Network Service Life cycle Management) of ETSI TST007 draft v0.0.10. Due to the number of participating vendors and due the time constraints, only a subset of test cases from all possible test from this section were chosen. Our test was designed to verify interoperability of the most common NFV MANO deployment scenarios in a typical cloud provider. We categorized all tests in three main test areas: Network life cycle management, Network service and operation and scaling function.

All tests were performed according to the ETSI NFV MANO architectural framework as presented below.

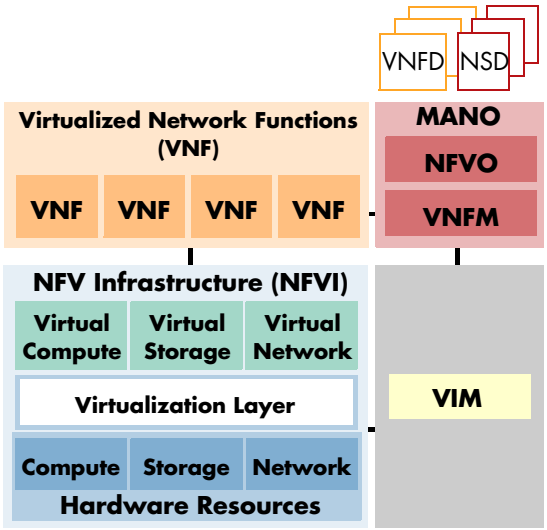


Figure 1: ETSI NFV MANO Architectural Framework

Test Preparation and Pre-Staging

The test preparation can be broken down into infrastructure installation, configuration, integration. The first three days were allocated to vendors for their hardware installation and software configuration. EANTC provided a comprehensive guide to participating NFVI vendors on how to setup the cloud environment. The test bed was designed taking into consideration secure multi-tenancy and management plane segregation. Virtual networks for data plane were carefully divided to allow consistent results and eliminate interference between parallel tests. Once this phase was completed, vendors immediately started the integration process. It is worth mentioning that during our test campaign, the Virtualized Infrastructure Manager (VIM) was provided by the NFVI vendors. During the integration phase, MANO and VIM/NFVI vendors completed the connection of their implementations and verified the proper access right and successful connectivity. We captured the progress of this process in a vendor readiness matrix.

We noticed that it was challenging to install the NFVI/VIM solutions and to integrate them with the MANO in a short time since in most cases, it is the first time for them to integrate with third party MANO. However, most of the vendors successfully managed to integrate their products with other vendors.

Interoperability Test Results

After one week of on-site testing and one week of remote testing, a total of 11 implementations were evaluated for interoperability, including three MANO solutions, four NFVIs platforms and four VNFs.

From a total of 324 maximum possible test combinations (9* MANO/NFVI combinations * 4 VNFs * 9 test cases) that could be done during our interoperability, we were able to complete 55 test combinations and report their interoperability results.

Test Equipment

For all test combinations we used either Spirent TestCenter or EANTC TestVNF to generate test traffic. The TestVNF is a Ubuntu-based Virtual Machine (VM), which is managed by automation software interfacing the NFVO/MANO northbound interface. The TestVNF can automatically report its network profile on booting and send bidirectional end-to-end traffic while receiving a remote call.

NETWORK SERVICE LIFE CYCLE MANAGEMENT

A fundamental and important functionality of the NFV MANO is the network service life cycle management. Life cycle management allows operators and cloud providers to optimally allocate resources based upon the actual operational requirement, thus preventing under-utilization of network resources. Image management of VNFs, network service instantiation – create network service using the NS on-boarding artefacts – and tear down of VNFs and network services (NS) using the NFV Orchestrator is the natural starting point. We tested interoperability between each MANO solution with the Virtual Infrastructure Manager (VIM) and the VNFs involved.

For each MANO-VNF-NFVI/VIM combination, we covered the following test cases:

Network Service Instantiation and Termination

VNFs and physical network functions can be combined and linked together inside a single network service construct. The network service descriptor (NSD) defines how the VIM-NFVI should allocate virtualized compute, storage and network resources to the network function components.

Interoperability requires precise definition of the interfaces exposed between the cloud's functional blocks: Due to the lack of a common standard, NFVO solutions represented descriptors in different formats. VNF vendors had to understand the VNF representation format for each NSD before being able to assist the NFVO vendors with the NSD creation.

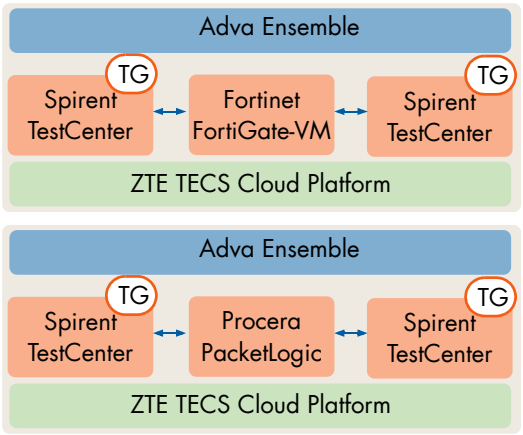
Additionally, VNF and NFVO vendors demand different methods to push the configuration and licenses towards the VNF instance. Vendor-specific requirements sometimes include special connectivity to licensing service or the Internet. This can be challenging in a distributed POP design.

The NS instantiation test started by triggering the process on the MANO user interface followed by verifying the activities on each of the functional blocks. For all participating VNFs – except for the Spirent CloudStress VNF – we used test traffic to verify the network forwarding function of the VNF component. We verified the successful instantiation of the network service by running an end-to-end functional test and by generating bidirectional traffic between the two EANTC provided virtual traffic generators. For Spirent CloudStress, VNF validation was done by generating CPU load and verifying via CloudStress application.

We used test traffic to verify the network forwarding function of the VNF component.

The NS termination test was triggered on the MANO solution. We verified that resources get terminated on the NFVI without errors.

Our team's test verification approach was in line with the test guidelines provided by ETSI. However, in some cases, manual operator intervention was unavoidable. Manual configurations were related to virtual network configurations since not all VIM-NFVI configurations were compatible with EANTC's test bed guidelines.



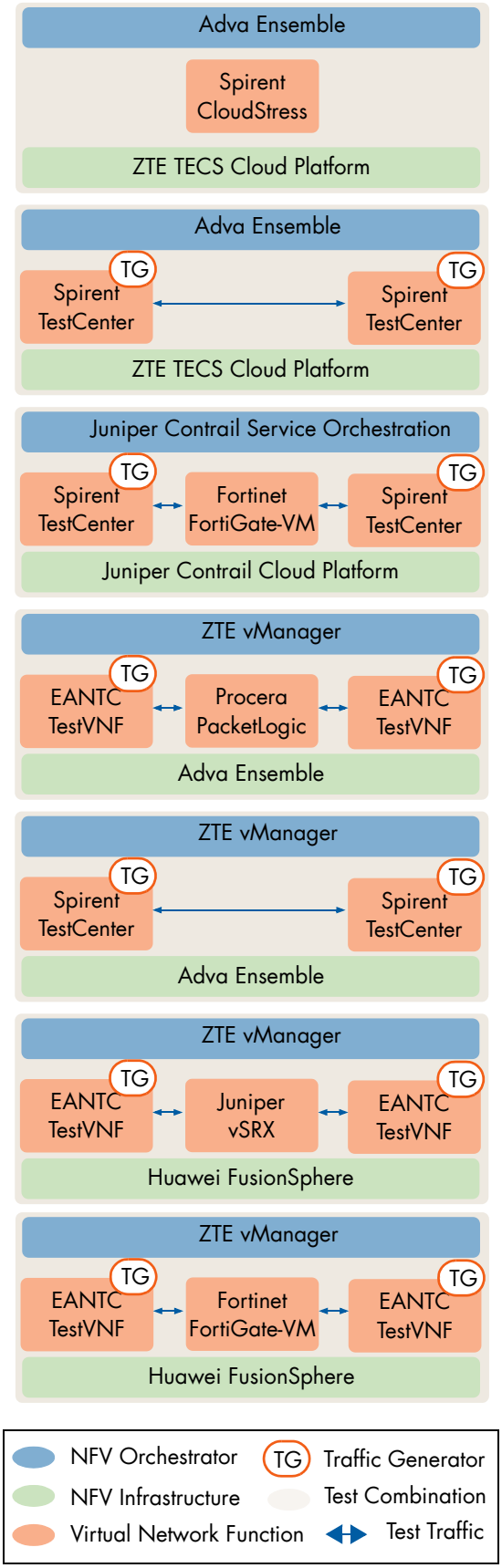


Figure 2: Network Service Instantiation/Termination

The following vendors successfully participated in this test: Adva, Juniper, ZTE as MANO; Adva, Huawei, Juniper and ZTE as NFVI; Fortinet, Juniper, Procera and Spirent acting as VNF. Figure 2 depicts the successful test combinations.

Work In Progress

At the time of the editorial deadline, some test combinations were still in progress and had already successfully completed the VNF package and NS on-boarding operations.

Since the focus of this test campaign was to evaluate interoperability between MANO, NFVI/VIM and VNF solutions we wanted to show these results too although they were not completed.

Figure 3 shows the work in progress combinations where virtualized resource orchestration was successful.

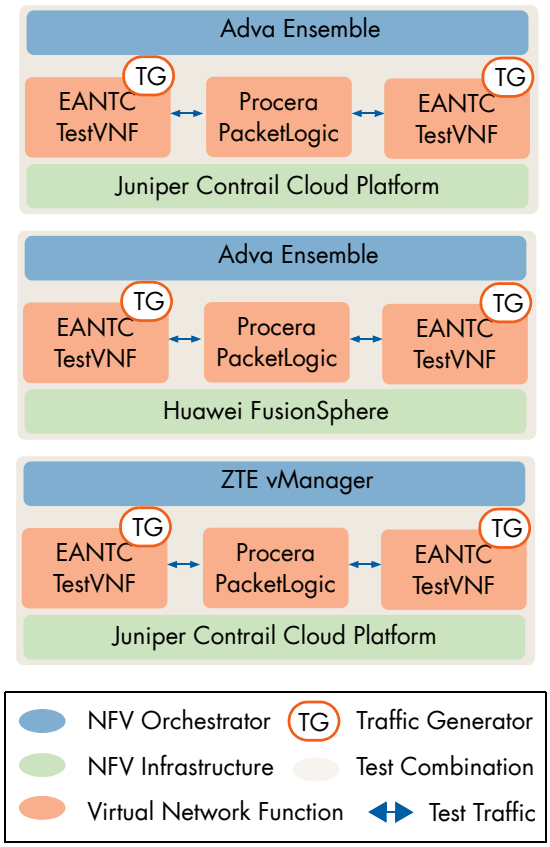
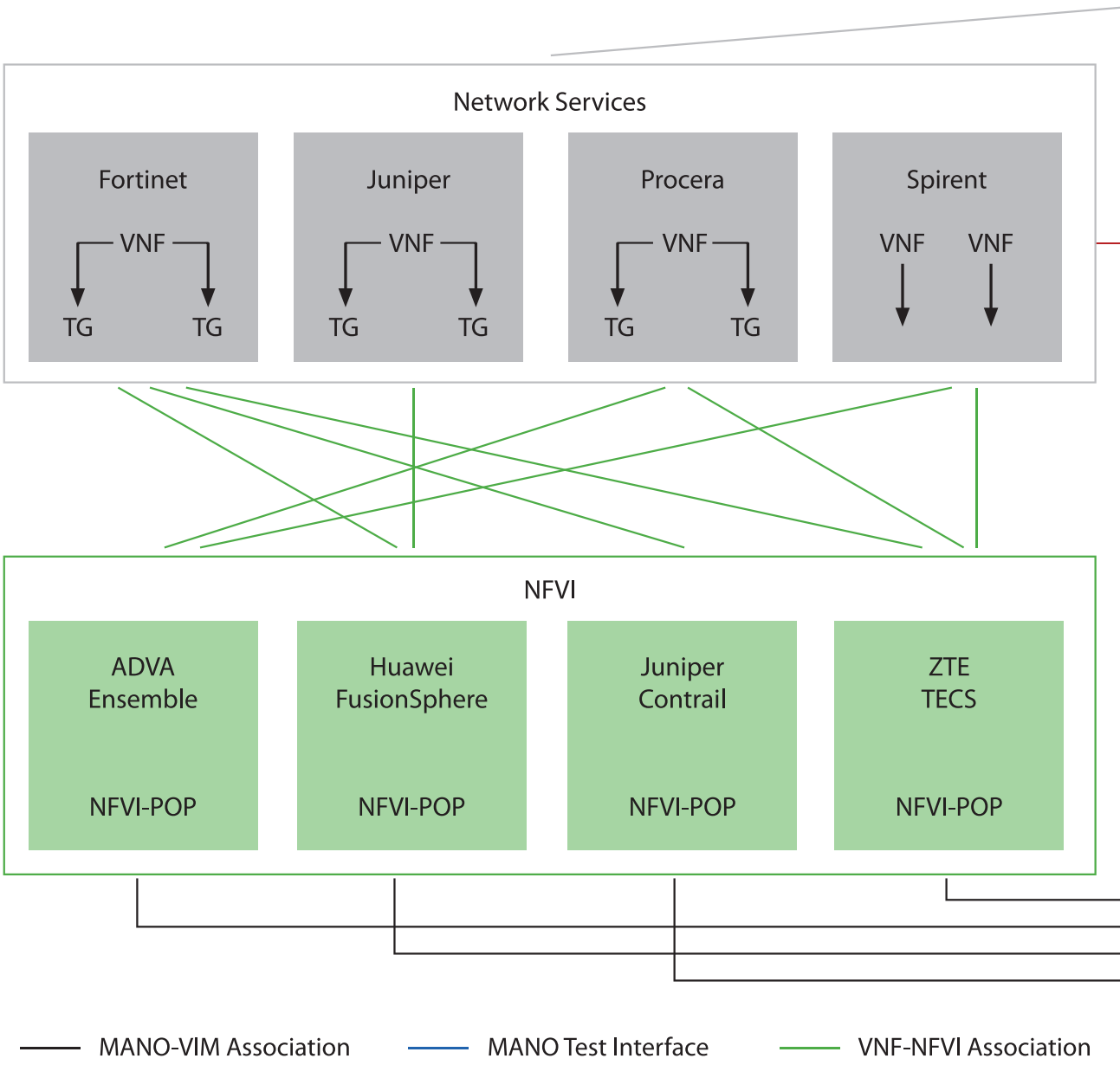
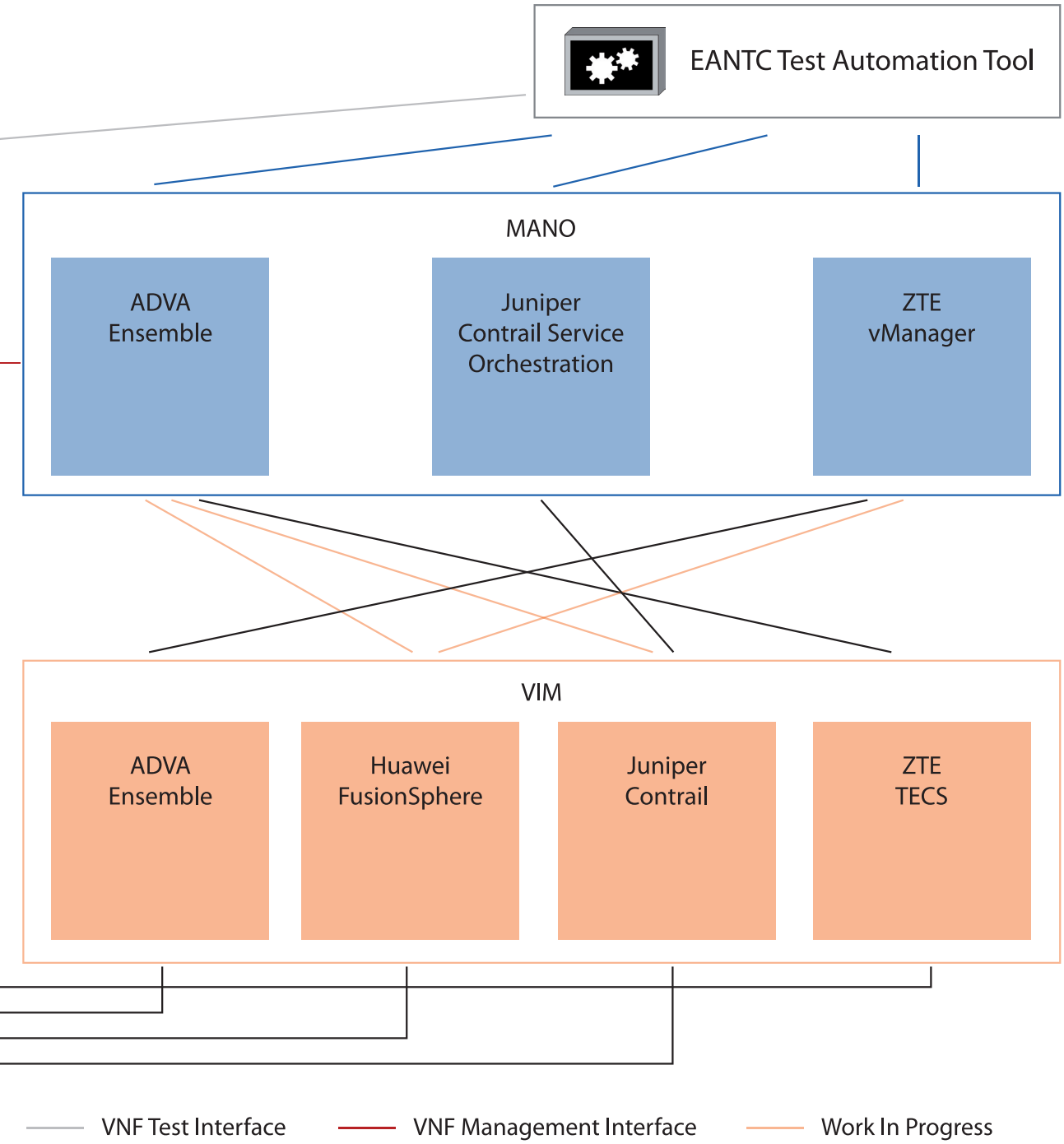


Figure 3: Work In Progress


Network Services
Fortinet
VNF
TG
TG
Juniper
VNF
TG
TG
Procera
VNF
TG
TG
Spirent
VNF
VNF
NFVI
ADVA Ensemble
NFVI-POP
Huawei FusionSphere
NFVI-POP
Juniper Contrail
NFVI-POP
ZTE TECS
NFVI-POP
MANO-VIM Association
MANO Test Interface
VNF-NFVI Association


EANTC Test Automation Tool
MANO
ADVA Ensemble
Juniper Contrail Service Orchestration
ZTE vManager
VIM
ADVA Ensemble
Huawei FusionSphere
Juniper Contrail
ZTE TECS
VNF Test Interface
VNF Management Interface
Work In Progress

NETWORK SERVICE OPERATIONS

Once the network service is instantiated and is running, it is important to evaluate the interoperability of its basic operations, such as stop/start of VNF as part of a network service update.

Network Service Update: VNF Stop/Start

As part of the network service update, an NFV MANO should be able to stop a VNF instance without releasing the virtualized resources that have been allocated to the VNF instance. A VNF instance whose application is faulty could be stopped as part of a fault management procedure.

Under certain scenarios, such as application failure, operators require to start a VNF that was previously in the stop state without having to modify the virtualized resources that were previously instantiated.

ZTE successfully participated in the test as MANO. The following vendors acted as NFVI/VIM: Adva and Huawei. Fortinet, Juniper, Procera and Spirent took part in the test as VNF vendors.

Initially, we requested MANO to instantiate a network service composed of VNF, VNF forwarding graph and virtual links as depicted in Figure 4. In all test combinations, a single virtual machine (VM) was used to realize a single VNF. We refer to a single VM component of the VNF as VNF Component (VNFC).

The ZTE vManager demonstrated the required functionality by stopping and starting each VNF component in the VNF. We triggered the VNF stop on the MANO and observed that the VNFC was shut down on the participating NFVI/VIM.

After we started VNF again, the VIM/NFVI showed the status of the VNF as started. Test traffic was correctly forwarded through the VNF instance.

In the case that the VNF is composed by several VNFCs, in order to stop the VNF, MANO is required to repeat the stop procedure for each VNFC. We also verified that the VNFC correctly started after receiving a new start command from MANO.

During this test, we observed that, while some vendors were able to stop individual VNFC of their VNF, other vendors could only perform the NS level stop operation, but not the VNF level operation, thus preventing them to execute these tests.

Figure 4 depicts the four test combinations that successfully participated in this test.

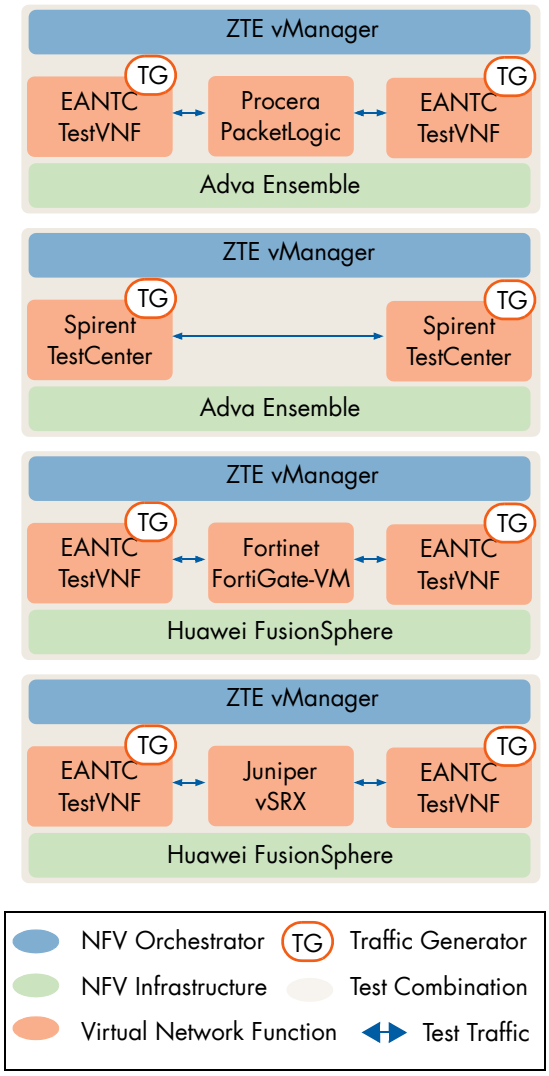


Figure 4: VNF Stop/Start

SCALING FUNCTIONS

An elastic response to changing resource requirements is a major aspect and benefit of virtualized network services. This elasticity is one of the main driver for virtualized environment compared to traditional server architectures. Scaling can be classified as either network service scaling out/in or VNF scale in/out.

In the life cycle of the network service, the NS and VNF could be scaled in/out based on either auto-scaling policy, VIM notification, VNF element management request or an operator action sent by MANO.

In our interoperability tests, to scale out/in the VNF deployed in the cloud, we used operator triggers to invoke the action.

Network Service Scale Out/In with an Operator Action

In the cloud computing environment elasticity is becoming a growing need due to the dynamic nature of different workloads. Network service scale out as part of horizontal scaling, refers to the ability of the MANO to add one or more instances, such as VNFs in response to the actual compute resource usage. On the other hand network service scaling in is the ability of the MANO to remove the existing VNFs.

The following devices participated as MANO: Adva Ensemble, Juniper Contrail Service Orchestration and ZTE vManager. Adva Ensemble, Huawei FusionSphere, Juniper Contrail Cloud Platform and ZTE TECS participated as NFVI/VIM. Fortinet FortiGate-VM, Juniper vSRX, Procera PacketLogic and Spirent TestCenter acted as VNF.

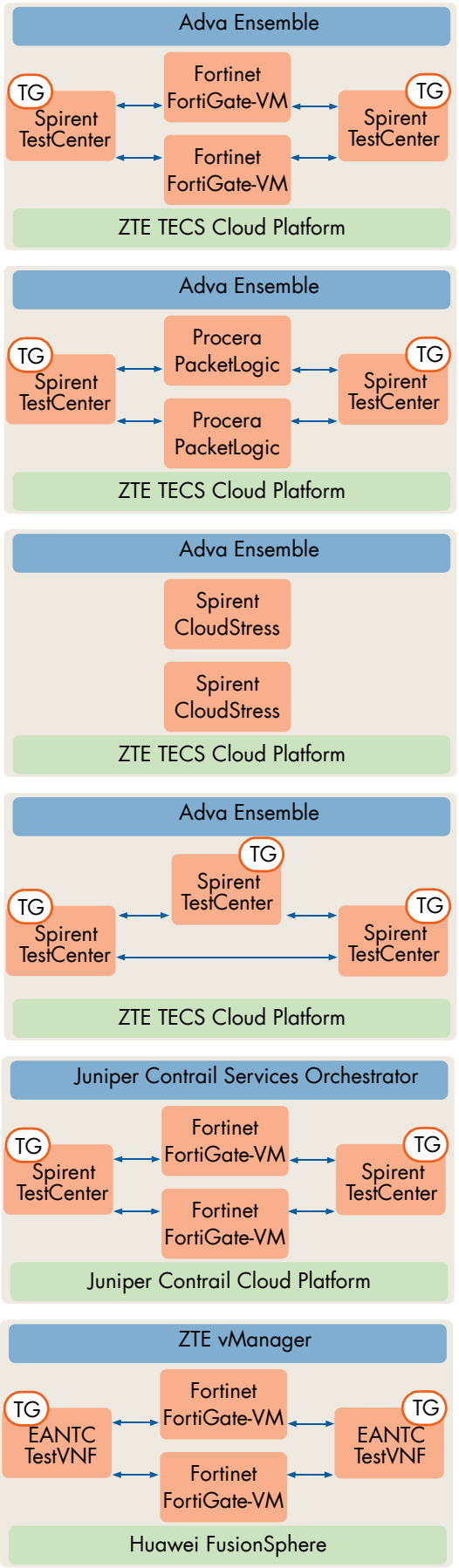
We started the test by verifying the correct instantiation of the NS. Two traffic generators, which were part of the NS, were connected to the left and right subnets separately attached to the data plane interfaces of the VNF. For all VNFs, except the Spirent CloudStress VNF, we validated the end-to-end connectivity of the network service by generating test traffic between the two traffic generator and verifying that the test traffic was forwarded through the NS without loss. For Spirent CloudStress, VNF validation was done by generating CPU load and verifying via CloudStress application.

Once this was done, we used an operator action to instruct the MANO to scale out the NS by adding an additional VNF. We expected an additional VNF to be instantiated and added into the existing NS parallel to the initial VNF.

In all test combinations shown in Figure 5, we successfully performed the NS scale out/in by adding/removing a VNF instance.

During the tests, we observed that vendors did not have an operator button to trigger NS scale in/out based on pre-defined flavor. Instead, they achieved this action by adding or removing VNFs on the existing network service descriptor.

Since the NS did not contain load balancing functions, we adjusted IP traffic to load the scaled out instances. This was not possible with layer 2 VNF components hence we verified the data plane frame count on their inbound and outbound interfaces instead.



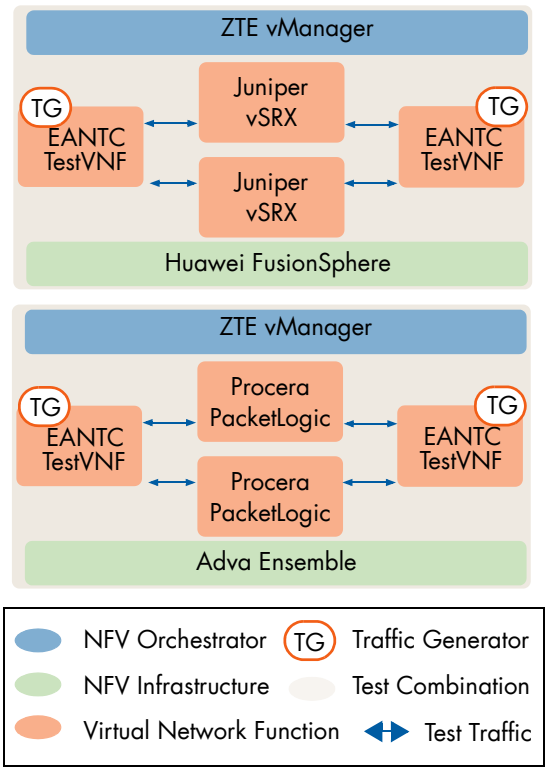


Figure 5: Network Service Scale Out/In

Another issue that was encountered during this test is that some vendors cannot add multiple links between two networks. Hence the additional VNF was chained between one of the existing traffic generators and a new one.

Network Service VNF Scale Out/In

Under certain scenarios, such as traffic overloading, an operator may increase the amount of resource used for providing the service. Conversely an operator may reduce the amount of resources used by service when there is no overloading condition.

VNF scaling out/in refers to the ability of MANO to add/remove one or more VNF component instances inside of the VNF. Since the participating functions were provided as a single VNFC, we verified that the MANO solution was capable of scaling out the same VNFC inside the VNF descriptor.

The test setup was straightforward and consisted of two traffic generators connected to the right and left subnet of the VNF. After we verified that the test traffic was forwarded through the VNFC without loss, we used an operator action to instruct the MANO to scale out the VNF by adding an additional VNFC. We expected the additional VNFC to be instantiated and added into the existing VNF. After we generated test traffic to verify the end-to-end connectivity, we observed that the traffic traversed through the additional VNFC.

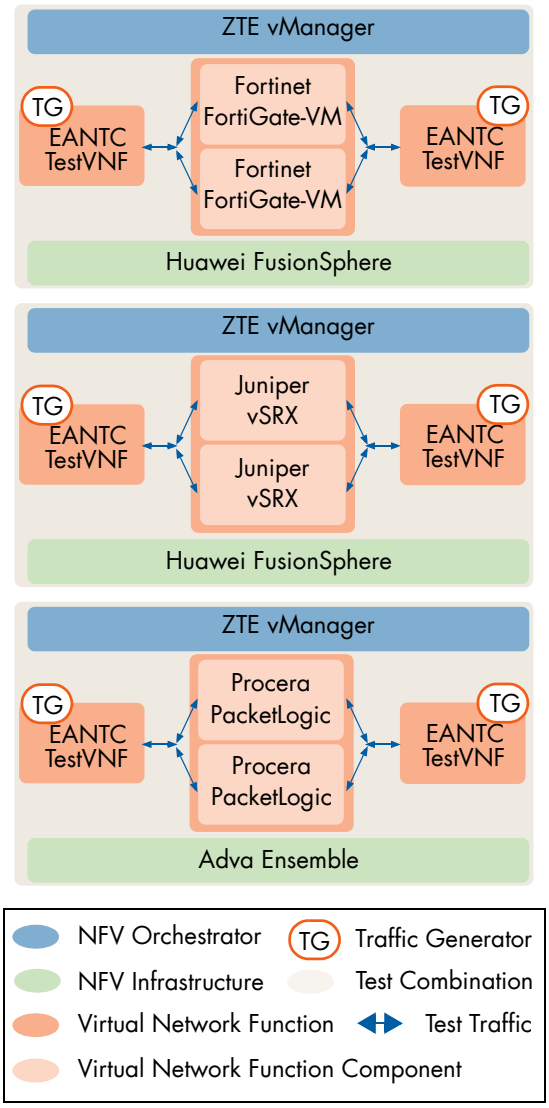


Figure 6: NS VNF Scale Out/In

In our interoperability test, VNF scale in/out was manually triggered by an operator action.

We observed during the test that, since all the participating VNF contained a single VNFC instance, a second component was re-created during the scale out operation from the original VNFC in order to achieve the required functionality.

The following vendors successfully participated in this test: ZTE participated as MANO, Adva and Huawei as NFVI/VIM and EANTC TestVNF as VNF.

Since the NS contained no load balancing functions, we adjusted IP traffic to load the scaled out instances. This was not possible with layer 2 VNF components hence we verified the data plane frame count on their inbound and outbound interfaces instead.

Network Service Healing with an Operator Action

One of the most critical aspects for any carrier grade NFV deployment is reliability. Complete healing network service composed of VNFs deployed in the cloud is an important requirement for any NFV deployment. We evaluated NS healing with an operator action.

Healing can either be done manually, requiring an operator's intervention, or automatically using thresholds and indicators. In this campaign we choose the first method for many reasons, with the most obvious being that the latter requires closer integration levels with the VNF instances.

To execute this test we shut down the VNFCs on the VIM. Once the target service was stopped, we activated the healing trigger on the MANO solution. Following the trigger we ensured that the service was restored on the VIM and VNF levels.

While pre-staging this test we realized a major difference in how MANO vendors implemented manual NS healing. While some vendors enabled and disabled automatic healing on a system-wide parameter, other vendors manually activated their VNFC. Some other vendors implemented a per service trigger, which applied to that service only.

The following combinations were verified to have successfully passed this test: Adva Ensemble, Juniper Contrail Service Orchestration and ZTE vManager acting as MANO; Adva Ensemble, Huawei FusionSphere, Juniper Contrail Cloud Platform and ZTE TECS Cloud Platform participated as NFVI, Fortinet FortiGate-VM, Juniper vSRX, Procera PacketLogic and Spirent TestCenter acting as VNF.

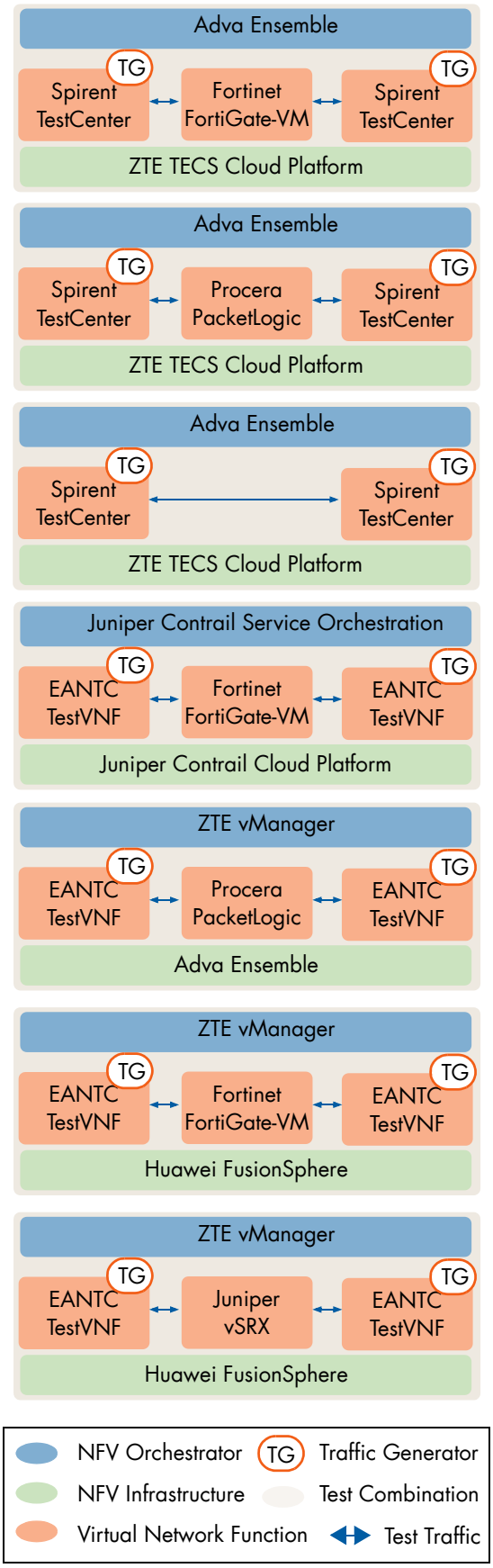


Figure 7: NS Healing

EANTC AG
European Advanced Networking Test Center

Salzufer 14
10587 Berlin, Germany
Tel: +49 30 3180595-0
info@eantc.de
http://www.eantc.com

New IP Agency

PO Box 1953
New York, NY 10156, USA
Tel: +1 301 502 9141
info@newipagency.com
http://www.newipagency.com

This report is copyright © 2017 EANTC AG and New IP Agency.
While every reasonable effort has been made to ensure accuracy and completeness of this publication, the authors assume no responsibility for the use of any information contained herein.
All brand names and logos mentioned here are registered trademarks of their respective companies in the United States and other countries.
20170522 v2.0